Cuatro vulnerabilidades de seguridad han sido descubiertas en el software de monitoreo de flotas de cajeros automáticos ScrutisWeb, desarrollado por Iagona. Estas vulnerabilidades podrían ser aprovechadas para acceder a cajeros automáticos de manera remota, subir archivos arbitrarios e incluso reiniciar los terminales.

El equipo de Synack Red Team (SRT) descubrió estas debilidades durante un compromiso con un cliente. Las problemáticas han sido solucionadas en la versión 2.1.38 de ScrutisWeb.

> *«La explotación exitosa de estas vulnerabilidades podría permitir que un atacante suba y ejecute archivos arbitrarios»,* informó la Agencia de Ciberseguridad e Infraestructura de Estados Unidos (CISA) en un aviso publicado el mes pasado.

ScrutisWeb es una solución basada en navegador para monitorear flotas de cajeros automáticos en el ámbito bancario y minorista. Esto incluye obtener información sobre el estado del sistema, detectar alertas de falta de papel, apagar o reiniciar un terminal y modificar datos de manera remota.

Los detalles de las cuatro fallas son los siguientes:

- CVE-2023-33871 (puntuación CVSS: 7.5) – Una vulnerabilidad de recorrido de directorios que podría permitir a un usuario no autenticado acceder directamente a cualquier archivo fuera de la raíz del servidor.

- CVE-2023-35189 (puntuación CVSS: 10.0) – Una vulnerabilidad de ejecución remota de código que podría permitir a un usuario no autenticado subir un archivo malicioso y ejecutarlo.

- CVE-2023-35763 (puntuación CVSS: 5.5) – Una vulnerabilidad criptográfica que podría permitir a un usuario no autenticado descifrar contraseñas encriptadas en texto plano.

- CVE-2023-38257 (puntuación CVSS: 7.5) – Una vulnerabilidad de referencia directa a objetos insegura que podría permitir a un usuario no autenticado ver información de perfil, incluyendo nombres de inicio de sesión de usuario y contraseñas encriptadas.

La vulnerabilidad más seria es CVE-2023-35189, ya que permite a un usuario no autenticado subir cualquier archivo y luego visualizarlo nuevamente desde un navegador web, lo que resulta en una inyección de comandos.

En un escenario hipotético de ataque, un adversario podría aprovechar CVE-2023-38257 y CVE-2023-35763 para acceder a la consola de administración de ScrutisWeb como administrador.

> *«Desde aquí, un actor malicioso podría monitorear las actividades en cajeros automáticos individuales dentro de la flota. La consola también permite poner cajeros automáticos en modo de administración, subir archivos, reiniciarlos y apagarlos por completo»,* mencionó Synack.

Además, CVE-2023-35189 podría ser utilizado para eliminar archivos de registro en ScrutisWeb y ocultar las acciones.

> *«Esta vulnerabilidad podría ser aprovechada adicionalmente como punto de acceso en la infraestructura del cliente, convirtiéndola en un punto de pivote accesible desde internet para un actor malintencionado»,* afirmaron los investigadores.